(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
24 juillet 2003 (24.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/060841 A1

(51) Classification internationale des brevets[7] : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR03/00112

(22) Date de dépôt international :
15 janvier 2003 (15.01.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/00569 17 janvier 2002 (17.01.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6, place d'Alleray, F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants *(pour US seulement)* : **CANARD, Sébastien** [FR/FR]; 4, résidence Olympia, F-14000 Caen (FR). **GIRAULT, Marc** [FR/FR]; 4, rue Viviane, F-14000 Caen (FR). **TRAORE, Jacques** [FR/FR]; 14, rue Emile Dron, F-61100 Flers (FR).

(74) Mandataire : **JEUNE, Pascale**; France Telecom R & D/VAT/VPI, 38-40, rue du Général Leclerc, F-92794 Issy Moulineaux Cedex 9 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Publiée :**

— *avec rapport de recherche internationale*
*avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

(54) Title: CRYPTOGRAPHIC REVOCATION METHOD USING A CHIP CARD

(54) Titre : PROCEDE CRYPTOGRAPHIQUE DE REVOCATION A L'AIDE D'UNE CARTE A PUCE

(57) Abstract: The invention relates to a cryptographic method and to a chip card which is used to carry out said method. The inventive cryptographic method comprises the following steps: before any calculation is performed by a computing means of the chip card, said chip card reads (2) an integral list, in a storage means of a second entity, of identifiers of first proprietary entities of a chip card, said list being linked to each status assigned to each of the first entities by the second entity; and, subsequently, the chip card compares (3) the identifier stored in a storage means of the chip card with the contents of the list, in order to authorise (5) or prohibit (4) any calculation by the computing means depending the result of said comparison.

(57) Abrégé : La présente invention se rapporte à un procédé cryptographique et à une carte à puce pour la mise oeuvre du procédé. Le procédé cryptographique consiste avant tout calcul par un moyen de calcul de la carte à puce, à lire (2) par la carte à puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale de premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité, à comparer (3), par la carte à puce, l'identifiant mémorisé dans un moyen de mémorisation de la carte à puce et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen de calcul en fonction du résultat de la comparaison.

WO 03/060841 A1

# PROCEDE CRYPTOGRAPHIQUE DE REVOCATION A L'AIDE D'UNE CARTE A PUCE

Domaine de l'invention

La présente invention se rapporte au domaine des télécommunications et plus particulièrement à la sécurisation des transmissions, en particulier pour des services, qui fait appel à la cryptographie.

Etat de l'art

Pour authentifier l'origine d'un document transmis par des moyens de télécommunication, il a été développé des mécanismes de signature électronique. Il faut noter que les termes transmission sous forme électronique sont couramment utilisés pour qualifier une transmission d'un document par des moyens de télécommunication. Les documents dont il est question dans le contexte de l'invention se présentent obligatoirement sous forme numérique par opposition à une présentation sous forme papier ; le terme message est utilisé dans la suite de la demande pour désigner ce type de document. Les mécanismes de signature électronique les plus courants reposent sur des techniques de cryptographie dites à clé publique qui mettent en jeu une entité dite autorité de confiance. Habituellement, cette autorité de confiance génère des certificats pour le compte d'utilisateurs des procédés courants à clé publique ; ces certificats établissent un lien entre une clé publique et l'identité du propriétaire de cette clé. Pour mettre en œuvre un tel procédé, l'individu signataire du message doit préalablement se faire certifier auprès de l'autorité de confiance en lui communiquant au moins sa clé publique et son identité. Lors de sa mise en œuvre, le procédé de signature calcule une signature électronique du message en prenant en compte d'une part le contenu du message et d'autre part la clé privée de l'individu. Le signataire transmet au destinataire le message, la signature et son certificat. Le destinataire du message vérifie la signature électronique du message à l'aide d'au moins la clé publique et du contenu du message.

Pour des applications particulières, telles que le vote électronique, les enchères électroniques ou le paiement électronique anonyme, il est nécessaire de pouvoir disposer d'une signature électronique dite anonyme. Une signature électronique anonyme a les mêmes caractéristiques qu'une signature électronique sauf que le destinataire ne peut déterminer l'identité du signataire ; le signataire garde l'anonymat. Toutefois, le destinataire peut s'adresser à l'autorité de confiance qui dispose, par

l'intermédiaire du certificat, d'un moyen pour lever l'anonymat. Parmi les différents types de signature anonyme, il existe un type particulier appelé signature anonyme de groupe. Un procédé de signature anonyme de groupe permet à chaque membre d'un groupe de produire une signature électronique qui soit caractéristique du groupe. Le destinataire d'un message accompagné d'une signature anonyme de groupe peut vérifier que la signature a été produite par un des membres du groupe. Toutefois il ne peut déterminer, parmi les différents membres du groupe, le membre dont il s'agit.

Dans le contexte de l'invention, un groupe est un ensemble d'individus qui se déclarent auprès d'une autorité comme appartenant à un même groupe. Lors de cette déclaration, chaque individu interagit avec l'autorité de confiance selon un protocole déterminé à l'issue duquel l'individu obtient une clé privée, associée à une clé publique de groupe préalablement déterminée par l'autorité de confiance, et l'autorité et l'individu obtiennent un identifiant de l'individu associé à cette clé privée. Chacun de ces individus est dans la suite de la demande désigné par le terme de membre. Un exemple d'un tel protocole est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. La même interaction intervient lors de l'arrivée d'un nouveau membre. L'existence d'un groupe se traduit du côté de l'autorité de confiance par l'attribution au groupe d'une clé publique dite de groupe et par l'attribution à chaque membre d'une clé privée associée à la clé publique, différente pour chaque membre, et d'un identifiant. A l'aide de sa clé privée, un membre peut produire une signature anonyme de groupe d'un message de son choix. Un destinataire quelconque peut vérifier que cette signature a bien été produite par un des membres du groupe à condition d'utiliser la clé publique de groupe. A l'issue de la vérification, le destinataire a la certitude que la signature a été produite, ou pas, par un membre du groupe, mais il n'obtient aucune information sur l'identifiant de ce membre ; la signature est anonyme. Le destinataire a toutefois la possibilité de s'adresser à l'autorité de confiance qui peut déterminer l'identité du signataire à partir de l'identifiant chiffré, au moyen d'une clé publique de l'autorité de confiance, qui accompagne la signature anonyme de groupe. L'autorité de confiance peut donc lever l'anonymat à tout moment.

Après constitution auprès de l'autorité de confiance, un groupe peut évoluer. Selon un premier type d'évolution, de nouveaux individus peuvent devenir membres du groupe. Selon un deuxième type d'évolution, des membres peuvent disparaître, soit

par le départ d'un individu du groupe, soit par l'exclusion d'un individu du groupe ; pour ce type d'évolution, on parle de révocation. A chaque évolution du groupe, l'autorité de confiance est confrontée au problème de donner ou de retirer à un membre du groupe les moyens de produire une signature anonyme du groupe. Le premier problème posé, qui réside dans l'attribution des moyens de produire une signature anonyme du groupe à un nouveau membre, est résolu en utilisant un des algorithmes de génération de clé publique/clé privée connus qui permettent d'associer à une même clé publique autant de clés privés que nécessaire. Un exemple d'un tel algorithme est décrit dans l'article de J.Camenisch et M.Michels qui a pour référence "Efficient group signature signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997.

Art antérieur

Le second problème posé, qui réside dans le fait de retirer à un individu ces moyens, présente différentes solutions connues qui sont des procédés de révocation.

Un premier de ces procédés est décrit dans l'article suivant de E. Bresson et J. Stern, « Efficient Revocation in group Signatures », in K. Kim, editor, Public Key Cryptography – PKC 2001, volume 1992 of LNCS, pages 190-206, Springer-Verlag, 2001. Ce procédé repose sur le fait que chaque membre d'un groupe possède un identifiant qui lui est propre. Etant donné que la signature doit rester anonyme, il n'est pas possible de dévoiler cet identifiant. Toutefois, selon le procédé, l'identifiant du signataire est divisé par celui de chaque membre révoqué ; le résultat de la division est toujours différent de 1 si et seulement si le signataire n'est pas lui-même un membre révoqué. Ensuite, le procédé chiffre, avec un algorithme de chiffrement, chacun des résultats de ces divisions et transmet au destinataire ces résultats chiffrés accompagnés d'éléments déterminés. Le destinataire exploite les éléments déterminés et les résultats chiffrés pour vérifier d'une part que les divisions ont été correctement effectuées et d'autre part que tous les résultats sont différents de 1 ; c'est-à-dire pour s'assurer que la signature a été produite par un membre non révoqué.

Ce procédé a pour inconvénient de générer une signature anonyme de groupe dont la longueur et le temps de calcul augmentent proportionnellement au nombre de membres révoqués, étant donné qu'il y a autant de résultats chiffrés et d'éléments déterminés que de membres révoqués.

Un deuxième de ces procédés de révocation est décrit dans l'article de H.J. Kim, J.I. Lim et D.H. Lee qui a pour référence « Efficient and Secure Member

Deletion in Group Signature Schemes », In D. Won, editor. Information Security and Cryptology – ICISC 2000, volume 2015 of LNCS, pages 150 et s. Springer-Verlag 2000. Ce procédé consiste à utiliser trois clés supplémentaires en plus des clés nécessaires à la réussite de la signature de groupe : une clé privée de propriété pour chaque membre, une clé publique de propriété pour permettre à chaque membre de vérifier la validité de sa clé et une clé publique de renouvellement permettant à chaque membre de modifier sa clé privée de propriété à chaque fois qu'un membre rejoint ou quitte le groupe. Pour chaque nouveau membre et pour chaque révocation d'un membre, l'autorité de confiance modifie la clé publique de propriété et la clé de renouvellement. Chaque membre restant du groupe modifie sa propre clé privée de propriété à l'aide de la clé de renouvellement et vérifie sa validité grâce à la clé publique de propriété. Lors de la signature électronique d'un message, le membre signataire utilise sa clé privée de propriété. Ainsi, le destinataire peut vérifier la signature électronique à l'aide de la clé publique de propriété. Ce procédé a pour inconvénient d'être d'application particulière car il est prouvé sûre uniquement dans un schéma de signature de groupe particulier qui correspond à celui présenté dans l'article de J. Cameniseh, M. Michels, ayant pour référence « A group Signature Scheme with Improved Efficiency », In K. Ohta et D. Pei, editors, Advances in Cryptology – ASIACRYPT'98, volume 1514 of LNCS, pages 160-174. Springler-Verlag, 1998. En outre, ce procédé est désavantageux en ce qu'il impose des calculs à chaque membre à chaque fois qu'un membre rejoint ou quitte le groupe ; or, ces calculs peuvent devenir fréquents si la dynamique du groupe est importante.

Un des objectifs de l'invention est de remédier aux inconvénients des méthodes connues et précédemment décrites.

Exposé de l'invention

A cet effet, l'invention a pour objet un procédé cryptographique mis en œuvre par une carte à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce comprenant un moyen de mémorisation dans lequel sont mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte à puce et comprenant un moyen de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète. Le procédé cryptographique selon l'invention comprend les étapes qui consistent :

- avant tout calcul par le moyen de calcul de la puce de la carte à puce, à lire par la puce dans un moyen de mémorisation d'une seconde entité une liste

d'identifiants sous forme intégrale des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,

- à comparer par la puce l'identifiant mémorisé dans le moyen de mémorisation de la puce et le contenu de la liste, pour autoriser ou interdire tout calcul du moyen de calcul en fonction du résultat de la comparaison.

L'invention a en outre pour objet une carte à puce pour la mise en œuvre d'un tel procédé.

Le procédé selon l'invention consiste à interdire par la puce de la carte à puce tout calcul cryptographique implanté dans la puce, lorsque le propriétaire de la carte à puce est dans un état positionné à révoqué par la seconde entité. Dans le cas contraire, le propriétaire de la carte à puce est dans un état positionné à non révoqué, la puce autorise le calcul. La seconde entité, qui est typiquement une autorité de confiance, met à jour une liste des identifiants de chaque propriétaire de carte à puce dont l'état est révoqué ou non révoqué. Cette liste est mémorisée par la seconde entité dans un moyen de mémorisation connecté à un réseau de télécommunication. Ce moyen est accessible par la carte à puce via un lecteur de carte à puce associé à un ordinateur tel un ordinateur personnel, lui-même connecté au réseau de télécommunication.

Ainsi, un membre révoqué ne peut pas effectuer de calcul cryptographique s'il est révoqué. Si l'algorithme de cryptographie implanté dans la puce est un algorithme de calcul de signature anonyme, le propriétaire de la carte à puce ne peut pas signer un fichier au moyen de sa carte à puce s'il est révoqué.

Le procédé selon l'invention peut être réalisé de manière particulière ; certaines réalisations sont listées ci-après de façon non-exhaustive.

Selon une réalisation particulière, la liste comprend les identifiants des entités révoquées, dans ce cas la liste est dite liste noire.

Selon une autre réalisation particulière, la liste comprend les identifiants des entités non révoquées, dans ce cas la liste est dite liste blanche.

Selon une autre réalisation particulière, la liste est signée par la seconde entité ; la seconde entité calcule cette signature au moyen d'un algorithme de signature. Cet algorithme peut-être un algorithme asymétrique à clé publique tel que RSA, RSA étant les initiales des inventeurs Avant toute autorisation, la puce vérifie la validité de la signature. Dans le cas d'un algorithme de signature à clé publique, la puce vérifie la signature au moyen du même algorithme asymétrique en prenant comme argument

d'entrée la clé publique. Cette vérification permet d'authentifier la liste dans son ensemble et donc de vérifier son intégrité

Selon une autre réalisation particulière, chaque identifiant de la liste est associé à une valeur de comptage, chaque ensemble formé de l'identifiant et de la valeur de comptage associé étant signé par la seconde entité ; la liste comprend une valeur du nombre d'identifiants listés dans la liste ainsi que la signature de cette valeur. Chaque signature est calculée de la même manière que dans la réalisation précédente. Avant toute autorisation, la puce vérifie la validité de chaque signature. Cette vérification permet d'authentifier chaque identifiant de la liste, la valeur de comptage associé et la valeur lue du nombre d'identifiants. En outre, la puce incrémente un compteur à chaque lecture d'un identifiant en prenant en compte la valeur de comptage associée à l'identifiant lu puis elle compare ce compteur à la valeur authentifiée avant toute autorisation de calcul par la puce. Cette comparaison permet de vérifier l'intégrité du nombre d'identifiants lus.

D'autres caractéristiques et avantages de l'invention apparaîtront lors de la description qui suit et qui est faite en regard des figures suivantes annexées de modes particuliers de réalisation donnés à titre d'exemples non limitatifs.

Brève description des figures

La figure 1 est un organigramme d'un procédé cryptographique selon l'invention.

La figure 2 est un organigramme d'un premier mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 3 est un organigramme d'un deuxième mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 4 est un organigramme d'un exemple de mise en œuvre par une puce du deuxième mode de réalisation d'un procédé cryptographique selon l'invention.

La figure 5 est un schéma d'une carte à puce selon l'invention.

La figure 1 est un organigramme d'un procédé cryptographique selon l'invention.

Description détaillée de modes de réalisation de l'invention

Le procédé est mis en œuvre par une carte à puce d'un ensemble de cartes à puce appartenant chacune à une première entité. Chaque première entité, typiquement une personne physique, peut être différente pour chaque carte à puce. Chaque carte à puce est équipée d'une puce qui comprend un moyen de mémorisation et un moyen de calcul. Une clé secrète et un identifiant de la première entité propriétaire de la carte à

puce sont mémorisés dans le moyen de mémorisation. Un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète est implanté dans le moyen de calcul.

Cet algorithme de cryptographie peut tout aussi bien être un algorithme de calcul de signature de groupe, un algorithme de chiffrement ou un algorithme de déchiffrement.

Un exemple d'algorithme de calcul de signature de groupe est décrit dans l'article de J.Camenisch et M.Stadler qui a pour référence "Efficient group signature schemes for large groups", In B.Kaliski, editor, Advances in Cryptology – CRYPTO97, volume 1296 of LNCS, pages 410 à 424, Springer-Verlag, 1997. Une autre description est donnée dans l'article de J.Camenisch et M.Michels qui a pour référence "A group signature scheme with improved efficiency. In K.Ohta et D.Pei, editors, Advances in cryptology- ASIACRYPT'98, volume 1514 of LNCS, pages 160-174. Springer-Verlag, 1998. L'algorithme RSA peut être utilisé comme algorithme de chiffrement / déchiffrement.

Le procédé comprend plusieurs étapes ci-après décrites. Pour signer, chiffrer ou déchiffrer, la puce active le moyen de calcul qui calcule une donnée de sortie en fonction d'arguments d'entrée présentés en entrée de l'algorithme de cryptographie.

Avant tout calcul 1 par le moyen de calcul de la puce de la carte à puce, le procédé consiste à lire 2 par la puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale des premières entités propriétaires d'une carte à puce. De manière totalement équivalente, le procédé peut écrire dans la puce une liste lue dans le moyen de mémorisation d'une seconde entité. Dans la suite de la description, toute opération de lecture peut être remplacée de manière totalement équivalente par une opération d'écriture. La liste est liée à chaque état attribué à chacune des premières entités par la seconde entité ; l'état est positionné à révoqué ou non révoqué par la seconde entité. La liste contient soit les premières entités révoquées, il s'agit d'une liste noire, soit les premières entités non révoquées, il s'agit d'une liste blanche. La seconde entité mémorise cette liste dans un moyen de mémorisation qui est accessible via un réseau de télécommunication. Il peut s'agir d'un espace mémoire sur un serveur ou sur une mémoire de masse par exemple.

Le procédé consiste ensuite à comparer 3 par la puce l'identifiant mémorisé dans le moyen de mémorisation de la puce et le contenu de la liste. Si, à l'issue de la comparaison, la puce trouve que la première entité est révoquée alors la puce interdit 4 tout calcul du moyen de calcul. Par contre, si, à l'issue de la comparaison, la puce

trouve que la première entité est non révoquée alors la puce autorise 5 tout calcul du moyen de calcul.

Pour mettre en œuvre par une puce la comparaison, le processus est le suivant. La puce initialise un témoin à un. Elle compare successivement chaque identifiant lu à l'identifiant mémorisé dans la puce ; s'il n'y a pas identité la puce positionne le témoin à un sinon elle positionne le témoin à zéro. A l'issue de la comparaison entre chaque identifiant lu et l'identifiant mémorisé dans la puce, la puce interdit tout calcul du moyen de calcul si le témoin est à un. Par contre si le témoin est à zéro, la puce autorise tout calcul du moyen de calcul.

Un premier mode de réalisation d'un procédé cryptographique selon l'invention est illustré par la figure 2. Ce mode comprend les étapes décrites en regard de la figure 1, elles ne sont pas re-décrites, et des étapes complémentaires ci-après décrites. La puce lit 10 en outre, en même temps que la liste et dans la même zone mémoire, une signature de cette liste. La signature est préalablement calculée par un moyen de calcul de la seconde entité. Avant autorisation 5 par la puce de tout calcul du moyen de calcul, la puce vérifie 11 la validité de la signature pour authentifier la liste et pour vérifier son intégrité. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul, sinon elle autorise 5 le calcul.

Un deuxième mode de réalisation d'un procédé cryptographique selon l'invention est illustré par la figure 3. Ce mode comprend les étapes décrites en regard de la figure 1, elle ne sont pas re-décrites, et des étapes complémentaires ci-après décrites. La puce lit 12, 13, 14 en outre, en même temps que la liste et dans la même zone mémoire, une valeur de comptage associée à chaque identifiant, une signature pour chaque ensemble composé d'un identifiant de cette liste et d'une valeur de comptage associée, la valeur du nombre d'identifiants de cette liste ainsi qu'une signature de cette valeur. La signature de chaque identifiant et de sa valeur de comptage associée, la valeur du nombre d'identifiants et la signature de cette valeur sont préalablement calculées par un moyen de calcul de la seconde entité et mémorisées dans la même zone mémoire que la liste. La puce incrémente 15 un compteur à chaque lecture par la puce d'un identifiant en prenant en compte la valeur de comptage associée à l'identifiant, pour compter le nombre d'identifiants. Avant autorisation 5 par la puce de tout calcul du moyen de calcul, la puce vérifie 16, 17 la validité de chacune des signatures pour authentifier respectivement chaque identifiant de la liste et le nombre d'identifiants. Si une des signatures n'est pas valide, la puce interdit 4 le calcul.

A l'issue de la lecture de la liste des identifiants, la puce compare 18 la valeur de son compteur à la valeur lue du nombre d'identifiants. Si ces valeurs sont différentes, la puce interdit 4 tout calcul du moyen de calcul. Si ces valeurs sont identiques, la puce vérifie 17 la validité de la signature de la valeur du nombre d'identifiants.La figure 4 illustre une mise en œuvre par une puce de ce deuxième mode. La puce initialise 19 un témoin à un et un compteur à zéro. La puce lit 20 un identifiant de la liste et la valeur de comptage associée, lit leur signature et incrémente le compteur. La puce compare 21 le témoin à zéro. Si le témoin est différent de zéro, la puce compare 22 l'identifiant lu à l'identifiant mémorisé dans la puce ; s'il n'y a pas identité la puce positionne 23 le témoin à un sinon elle positionne 24 le témoin à zéro. A l'issue de la comparaison entre l'identifiant lu et l'identifiant mémorisé dans la puce ou si le témoin est égal à zéro, la puce vérifie 25 la validité de la signature de l'ensemble composé de l'identifiant lu et de la valeur de comptage associée. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul. Par contre si la signature est valide, la puce se met en attente de l'identifiant suivant ou 26, s'il n'y a plus d'identifiant dans la liste, la puce lit 27 la valeur du nombre d'identifiants et sa signature. La puce compare 18 la valeur du nombre d'identifiants avec la valeur de son compteur. Si ces valeurs sont différentes, la puce interdit 4 tout calcul du moyen de calcul, sinon la puce vérifie 17 la validité de la signature de la valeur du nombre lu. Si la signature n'est pas valide, la puce interdit 4 tout calcul du moyen de calcul. Par contre si la signature est valide, la puce teste 28 la valeur du nombre d'identifiants. Si le témoin est différent de un, la puce interdit 4 tout calcul du moyen de calcul ; le membre est révoqué. Sinon, la puce autorise 5 tout calcul du moyen de calcul.

La figure 5 illustre de manière schématique une carte à puce selon l'invention.

La carte 30 à puce est équipée d'une puce 31 qui comprend au moins un moyen 32 de mémorisation, un moyen 33 de calcul et un moyen 34 de lecture dans un moyen de mémorisation d'une seconde entité via un réseau de télécommunication et un moyen 35 d'autorisation du moyen de calcul.

Le moyen 32 de mémorisation mémorise une clé secrète et un identifiant d'une première entité propriétaire de la carte à puce.

Dans le moyen 33 de calcul est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète. Le moyen 33 de calcul est en liaison avec le moyen 32 de mémorisation.

Le moyen 34 de lecture permet de lire une liste d'identifiants dans le moyen de mémorisation d'une seconde entité, via un réseau de télécommunication. Le moyen 34

de lecture transmet les données lues au moyen 33 de calcul ou/et au moyen 35 d'autorisation par des liaisons avec chacun de ces moyens.

Le moyen 35 d'autorisation autorise tout calcul par le moyen 33 de calcul en fonction du résultat d'une comparaison entre l'identifiant et le contenu de la liste.

Une telle carte 30 à puce permet la mise en œuvre d'un procédé selon l'invention.

Une première application d'un procédé selon l'invention est le vote électronique. Le vote électronique se déroule en deux phases :

- une inscription sur une liste électorale auprès d'une autorité administrative,
- une opération de vote auprès d'une urne connectée via un réseau de communication à un serveur d'une administration des votes.

Lors de l'inscription, l'électeur obtient dans une carte à puce, une clé privée personnelle et une clé privée de groupe. La signature anonyme que peut produire l'électeur au moyen de sa carte à puce, et à partir de sa clé privée personnelle, est dite "corrélable". Ceci signifie que, dans le cas où l'électeur tenterait de signer de manière anonyme un second bulletin de vote en produisant une signature anonyme, ce bulletin serait rejeté par l'urne. En effet, la signature anonyme étant corrélable, l'urne est en mesure de vérifier qu'il s'agit d'une seconde signature anonyme.

Un électeur malveillant ne peut pas prétendre avoir perdu sa clé privée de groupe, en recevoir une autre et être en mesure de voter deux fois. En effet, la mise en œuvre d'un procédé selon l'invention permet de lui interdire l'utilisation de la première clé privée de groupe ; cette clé privée de groupe est mise à jour au moment où il déclare avoir perdu la première clé privée de groupe. Cette perte est gérée par la mise en œuvre d'un procédé selon l'invention comme une révocation du membre.

Une seconde application d'un procédé selon l'invention est un service d'enchères électroniques. Les enchères font appel à trois protagonistes : un serveur d'enchères, une autorité de confiance et un client. L'ensemble des clients forme un groupe dit groupe des clients. Un utilisateur désirant s'inscrire au groupe des clients doit s'adresser à l'autorité de confiance qui lui fournit sa clé privée personnelle dans une carte à puce. Il obtient ainsi le droit de produire une signature anonyme de groupe. Muni de ce droit, il peut signer à l'aide de sa carte à puce chacune de ses enchères de manière anonyme. Lors d'une enchère pour un certain produit, chaque membre du groupe des clients peut enchérir en signant un message contenant notamment le produit mis en vente et le montant de son enchère. Le serveur d'enchères peut vérifier l'appartenance au groupe et donc la validité de l'enchère en vérifiant la signature

anonyme de groupe. Le vainqueur est celui qui donne la dernière enchère avant l'adjudication. Le dernier message reçu par le serveur d'enchères est donc celui du vainqueur. Le serveur adresse alors ce message et la signature anonyme de groupe correspondante à l'autorité de confiance qui est la seule capable d'en lever l'anonymat et donc de déterminer l'identité physique de l'acheteur du produit mis aux enchères.

Les enchères mettent en jeu des groupes dynamiques : de nouvelles personnes peuvent chaque jour s'inscrire au groupe, un membre peut quitter le groupe ou être exclu pour fraude à tout moment. Il est donc indispensable de mettre en place un système de révocation pour empêcher qu'un membre révoqué ne puisse se servir de sa signature de manière frauduleuse. En effet, le membre révoqué pourrait continuer à utiliser sa clé pour participer aux enchères et fausser le bon déroulement de ces dernières par exemple en faisant monter le montant. Et, s'il prend soin de se retirer suffisamment tôt du processus de façon à ne pas remporter les enchères en question, alors cette fraude n'est pas détectée puisque seule l'identité du gagnant est finalement révélée. La mise en œuvre d'un procédé selon l'invention permet de résoudre le problème de révocation d'un ou de membre(s) du groupe.

Une troisième application d'un procédé selon l'invention est le paiement électronique. Elle met en jeu quatre protagoniste : un client, un commerçant, une banque et une autorité de confiance. Chaque client doit se faire identifier par le système et obtenir une clé privée de groupe mémorisée dans une carte à puce, avant de pouvoir effectuer sa première transaction. Pour effectuer un paiement, le client doit retirer des pièces électroniques auprès de sa banque. Les pièces qu'il retire sont anonymes grâce à l'utilisation d'un mécanisme dit de signature aveugle. La dépense d'une pièce C chez un commerçant se fait de la manière suivante : le client génère au moyen de sa carte à puce une signature de groupe portant sur les pièces C et transmet l'ensemble signature et pièces C au commerçant. Le commerçant vérifie la signature de la banque attachée à chaque pièce C et vérifie la signature de groupe. Si chacune des deux signatures est valide, le commerçant accepte la transaction. A un moment donné du jour, le commerçant transmet à sa banque les signatures et les pièces reçues en paiement pour virement à son compte. En cas de fraude, par exemple par la réutilisation d'une même pièce dans plusieurs transactions, la banque envoie la signature de groupe portant sur la pièce litigieuse à l'autorité de confiance afin qu'elle identifie le client indélicat et sanctionne le contrevenant.

Un mécanisme fiable de révocation des clés compromises est nécessaire afin d'éviter une fraude du type suivant : un client malhonnête signale à l'autorité de

confiance la perte de sa clé privée s et décline alors toute responsabilité pour les fraudes qui pourraient être commises avec s. Le client remet sa clé à son complice, lequel peut alors utiliser s pour signer les pièces c qu'il a légitimement retirées à la banque, puis les dépenser autant de fois qu'il le souhaite. Un procédé selon l'invention permet de résoudre le problème de la révocation des clés s.

## REVENDICATIONS

1. Procédé cryptographique mis en œuvre par une carte (30) à puce d'un ensemble de cartes à puce appartenant chacune à une première entité qui peut être différente pour chaque carte à puce, chaque carte à puce étant équipée d'une puce (31) comprenant un moyen (32) de mémorisation dans lequel sont mémorisés une clé secrète et un identifiant de la première entité propriétaire de la carte (30) à puce et comprenant un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète, caractérisé en ce qu'il comprend les étapes qui consistent :
   - avant tout calcul par le moyen (33) de calcul de la puce (31) de la carte (30) à puce, à lire (2) par la puce (31) dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale des premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité,
   - à comparer (3) par la puce (31) l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen (33) de calcul en fonction du résultat de la comparaison.

2. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) n'appartient pas à la liste.

3. Procédé cryptographique selon la revendication 1, dans lequel la liste comprend l'ensemble des premières entités dont l'état est positionné à non révoqué par la seconde entité et dans lequel l'autorisation (5) de calcul est donnée par la puce (31) uniquement si l'identifiant mémorisé dans le moyen (32) de mémorisation de la puce (31) appartient à la liste.

4. Procédé cryptographique selon l'une des revendications 1 à 3, comprenant en outre les étapes qui consistent :

- en même temps que la lecture (2) de la liste, à lire (10) une signature de cette liste par la puce (31) dans le moyen de mémorisation de la seconde entité, la signature ayant été préalablement calculée par un moyen de calcul de la seconde entité,
- avant autorisation (5) par la puce de tout calcul du moyen (33) de calcul, à vérifier (11) par la puce (31) la validité de la signature.

5. Procédé cryptographique selon l'une des revendications 1 et 2, comprenant en outre les étapes qui consistent :
   - en même temps que la lecture (2) de la liste, à lire (12) des signatures des identifiants de la liste par la puce (31) dans le moyen de mémorisation de la seconde entité, chaque identifiant ayant donné lieu à une signature préalablement calculée par un moyen de calcul de la seconde entité,
   - en même temps que la lecture (2) de la liste, à lire (13, 14) par la puce (31) dans le moyen de mémorisation de la seconde entité, une valeur du nombre d'identifiants listés dans cette liste ainsi qu'une signature de cette valeur, la valeur et sa signature ayant été préalablement calculées par un moyen de calcul de la seconde entité,
   - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de calcul, à vérifier (16, 17) par la puce (31) la validité de chacune des signatures,
   - à compter (15) par la puce (31) le nombre d'identifiants contenus dans la liste lue,
   - avant autorisation (5) par la puce (31) de tout calcul du moyen (33) de calcul, à vérifier (18) l'égalité entre la valeur du compteur et la valeur lue.

6. Carte (30) à puce pour la mise en œuvre d'un procédé selon l'une des revendications 1 à 5, caractérisée en ce qu'elle (30) est équipée d'une puce (31) qui comprend au moins :
   - un moyen (32) de mémorisation d'une clé secrète et d'un identifiant d'une première entité propriétaire de la carte à puce,
   - un moyen (33) de calcul dans lequel est implanté un algorithme de cryptographie ayant pour arguments d'entrée au moins la clé secrète,

- un moyen (34) pour lire une liste d'identifiants sous forme intégrale dans un moyen de mémorisation d'une seconde entité, via un réseau de télécommunication,
- un moyen (35) pour autoriser tout calcul par le moyen (33) de calcul en fonction du résultat d'une comparaison entre l'identifiant et le contenu de la liste.

*FIG. 1*

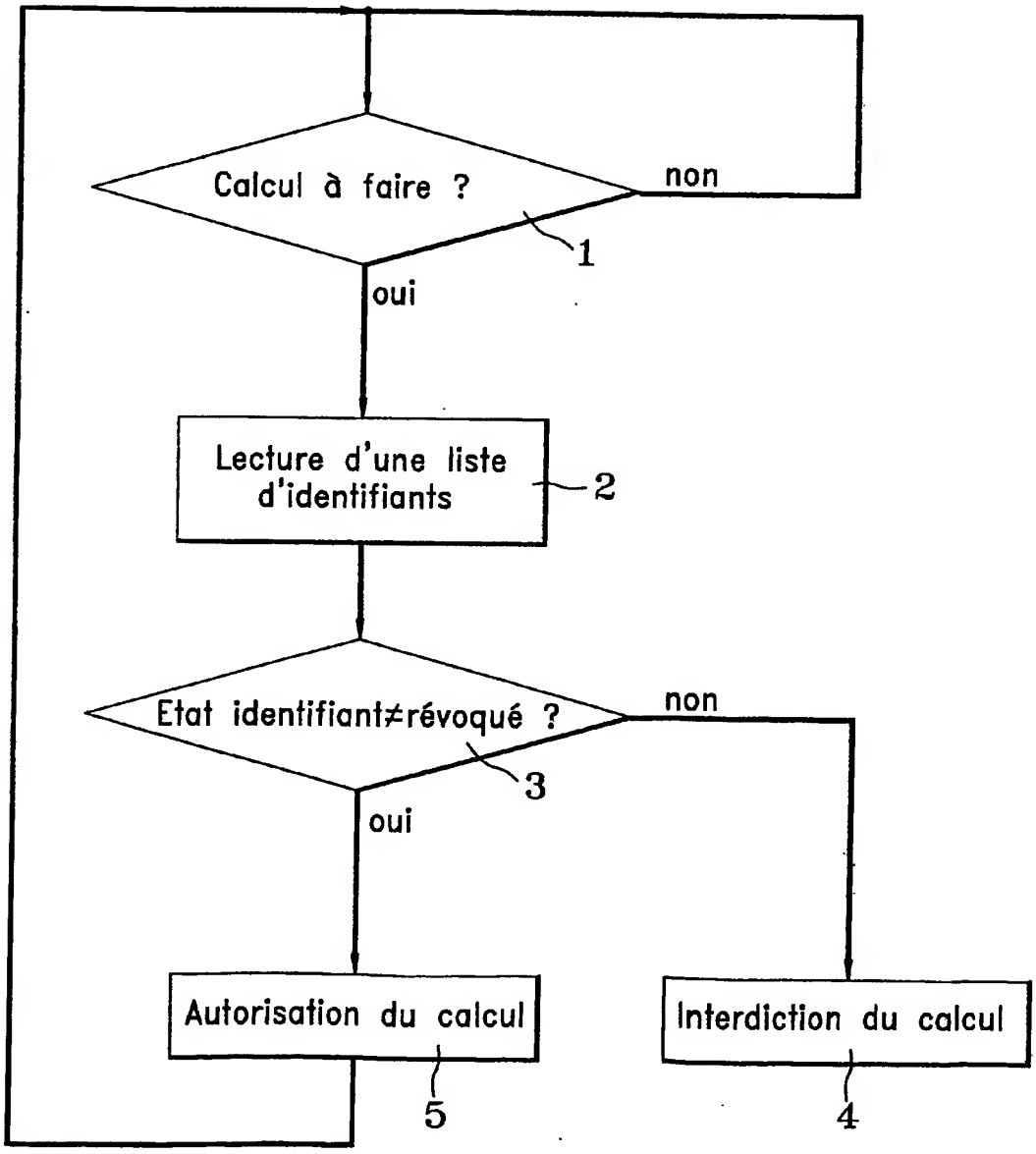
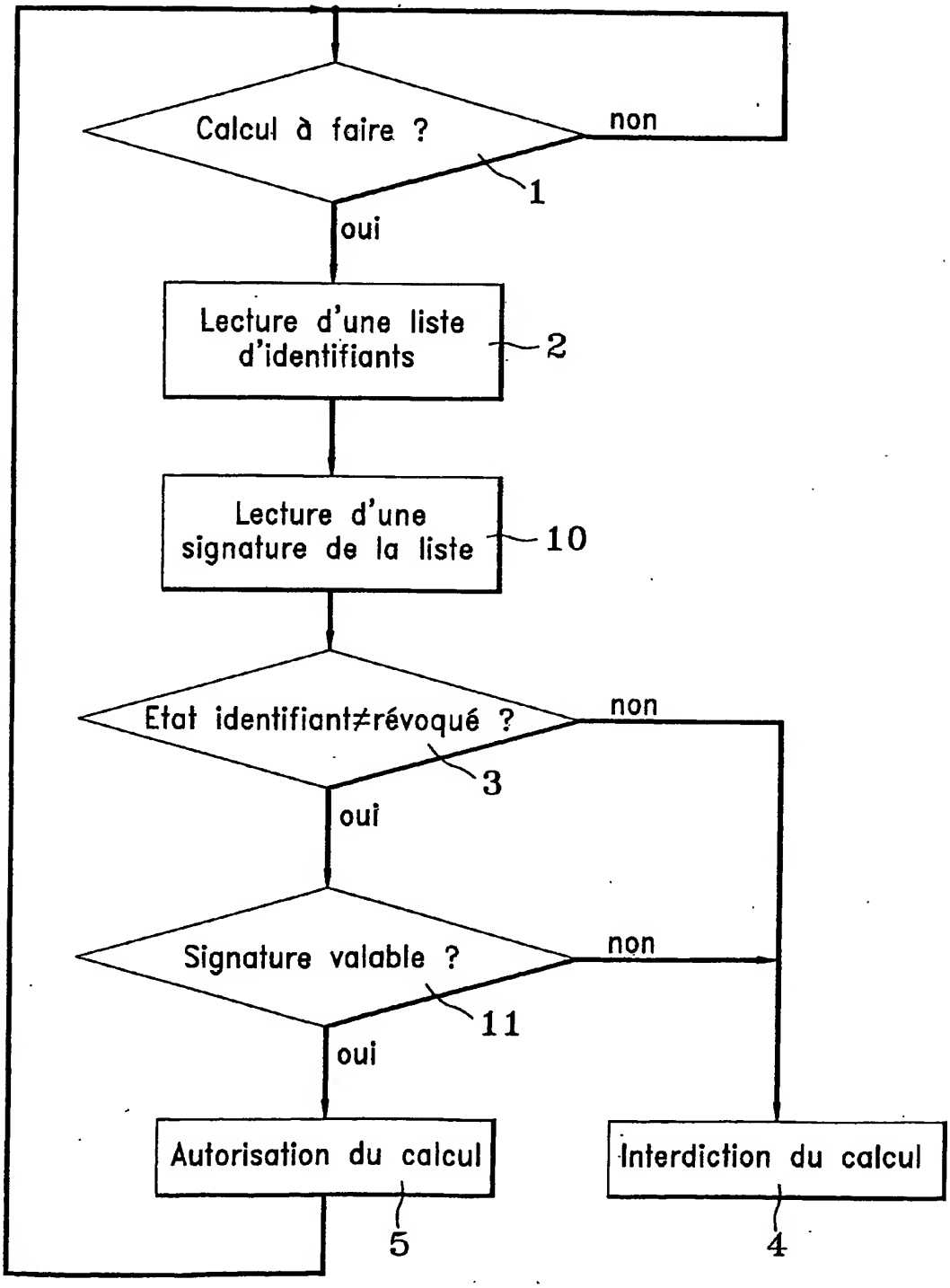

Calcul à faire ?
non
1
oui
Lecture d'une liste d'identifiants
2
Etat identifiant≠révoqué ?
non
3
oui
Autorisation du calcul
Interdiction du calcul
5
4

*FIG.2*


Calcul à faire ?
non
1
oui
Lecture d'une liste d'identifiants
2
Lecture d'une signature de la liste
10
Etat identifiant≠révoqué ?
non
3
oui
Signature valable ?
non
11
oui
Autorisation du calcul
5
Interdiction du calcul
4

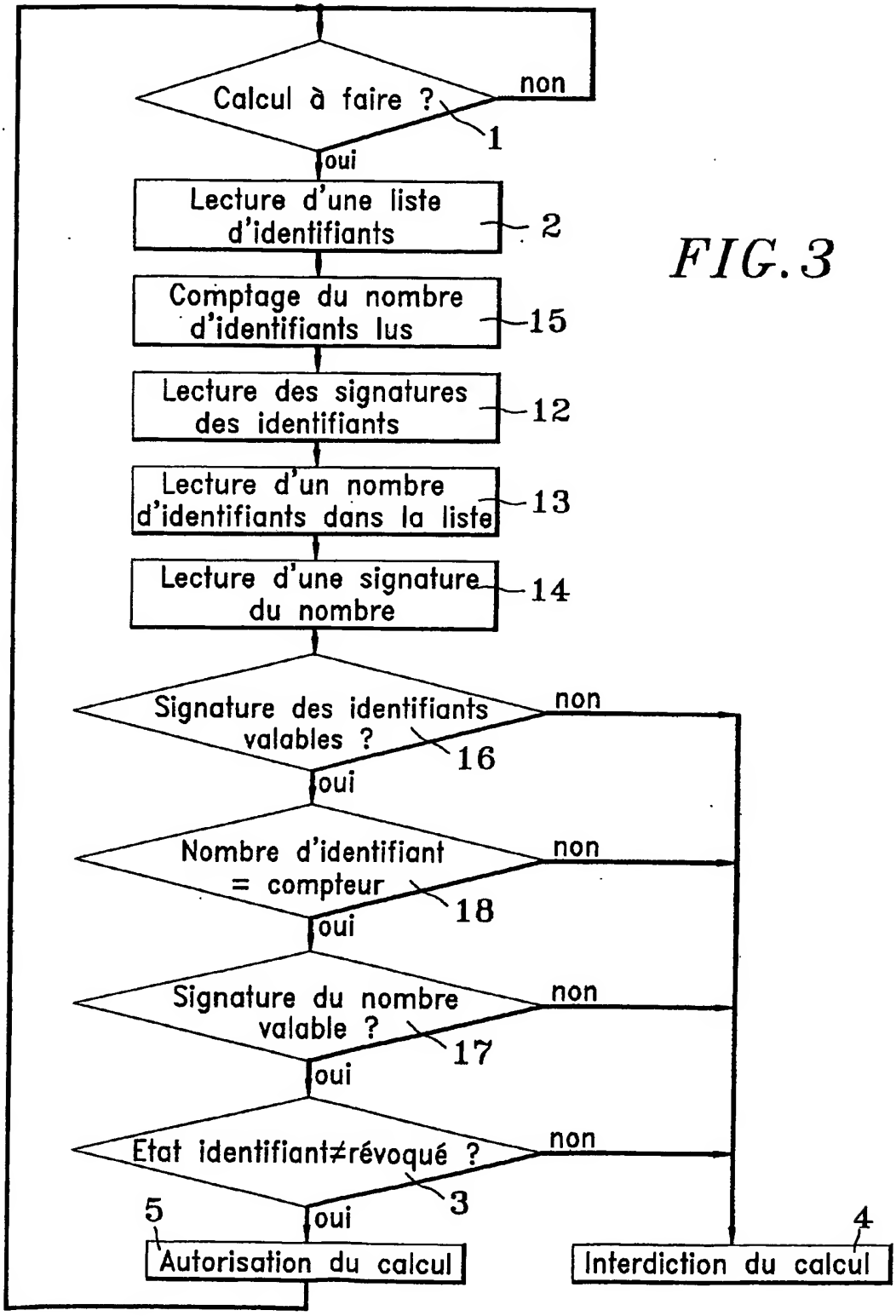

Calcul à faire ?
non
1
oui
Lecture d'une liste d'identifiants
2
Comptage du nombre d'identifiants lus
15
Lecture des signatures des identifiants
12
Lecture d'un nombre d'identifiants dans la liste
13
Lecture d'une signature du nombre
14
Signature des identifiants valables ?
non
16
oui
Nombre d'identifiant = compteur
non
18
oui
Signature du nombre valable ?
non
17
oui
Etat identifiant≠révoqué ?
non
3
5
oui
Autorisation du calcul
4
Interdiction du calcul

*FIG. 3*

FIG. 4

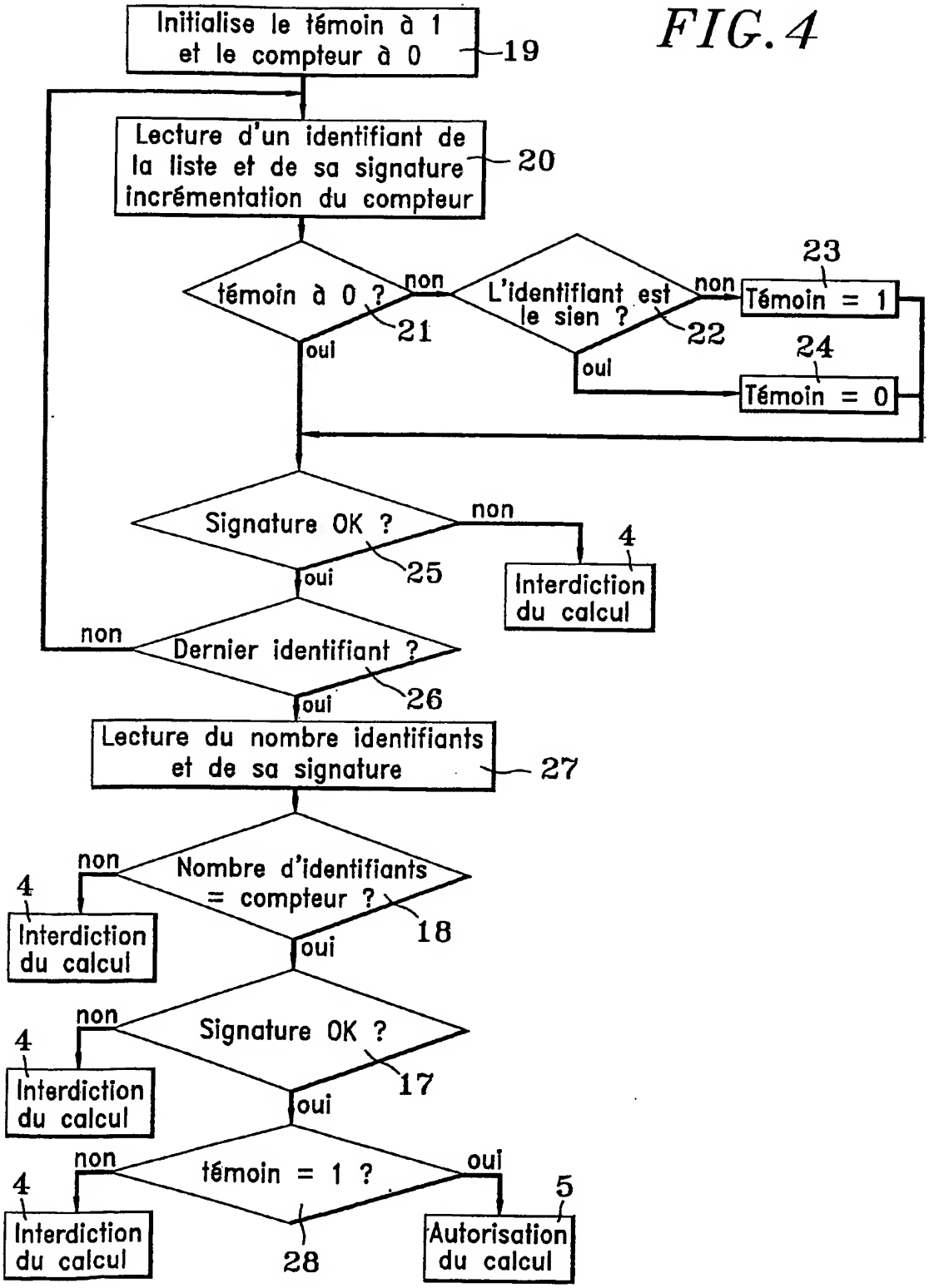
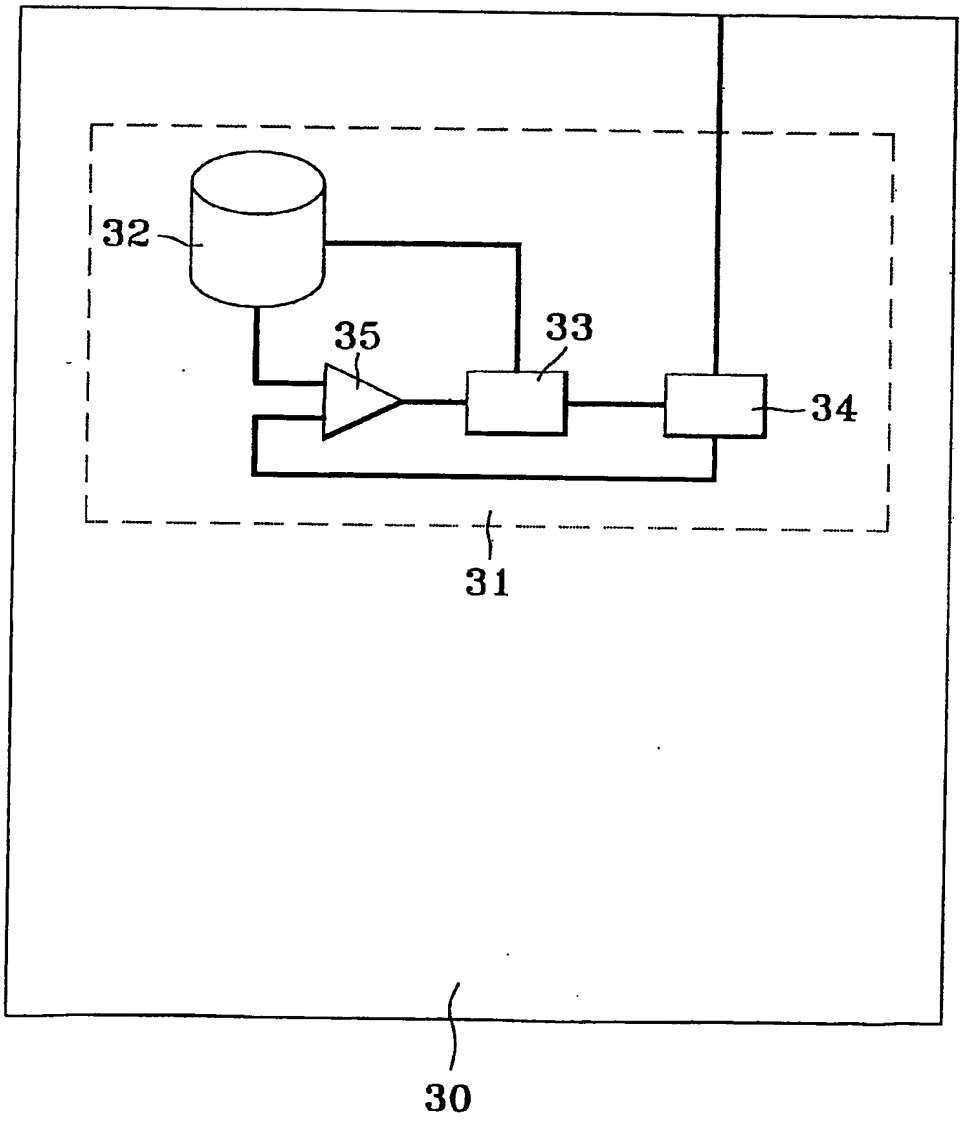

Initialise le témoin à 1 et le compteur à 0
19
Lecture d'un identifiant de la liste et de sa signature incrémentation du compteur
20
témoin à 0 ?
non
21
oui
L'identifiant est le sien ?
non
22
oui
23
Témoin = 1
24
Témoin = 0
Signature OK ?
non
25
oui
4
Interdiction du calcul
non
Dernier identifiant ?
26
oui
Lecture du nombre identifiants et de sa signature
27
non
Nombre d'identifiants = compteur ?
18
oui
4
Interdiction du calcul
non
Signature OK ?
17
oui
4
Interdiction du calcul
non
témoin = 1 ?
oui
28
4
Interdiction du calcul
5
Autorisation du calcul

*FIG. 5*



# INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/00112

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| X | US 5 191 193 A (LE ROUX JEAN-YVES)<br>2 March 1993 (1993-03-02)<br>abstract<br>column 1, line 24 -column 2, line 42<br>column 3, line 38 -column 4, line 51<br>column 5, line 30 - line 35<br>column 5, line 52 -column 6, line 2<br>figures 1,2 | 1,2,6 |
| Y | US 3 696 335 A (LEMELSON JEROME H)<br>3 October 1972 (1972-10-03)<br>abstract<br>column 2, line 23 -column 3, line 44<br>column 12, line 4 - line 15<br>figure 1 | 1-4,6 |

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

| Date of the actual completion of the international search | Date of mailing of the international search report |
|---|---|
| 15 May 2003 | 26/05/2003 |

| Name and mailing address of the ISA | Authorized officer |
|---|---|
| European Patent Office, P.B. 5818 Patentlaan 2<br>NL – 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Dujardin, C |

Form PCT/ISA/210 (second sheet) (July 1992)

## INTERNATIONAL SEARCH REPORT

International Application No
PCT/FR 03/00112

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

| Category * | Citation of document, with indication, where appropriate, of the relevant passages | Relevant to claim No. |
|---|---|---|
| Y | WO 00 08610 A (MICROSOFT CORP)<br>17 February 2000 (2000-02-17)<br>abstract<br>page 9, line 21 -page 11, line 3<br>page 11, line 24 -page 12, line 7<br>page 12, line 23 -page 19, line 2<br>figures 1-5 | 1-4,6 |
| A | EP 0 427 465 A (AMERICAN TELEPHONE & TELEGRAPH) 15 May 1991 (1991-05-15)<br>abstract<br>column 5, line 4 - line 50<br>column 6, line 54 -column 7, line 11<br>figure 1 | 1,2,6 |
| A | EP 0 378 349 A (VISA INT SERVICE ASS)<br>18 July 1990 (1990-07-18)<br>abstract<br>page 3, line 19 -page 4, line 12<br>page 5, line 22 - line 49<br>page 13, line 4 - line 20 | 1,2,6 |

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/FR 03/00112

| Patent document cited in search report | | Publication date | Patent family member(s) | | Publication date |
|---|---|---|---|---|---|
| US 5191193 | A | 02-03-1993 | FR | 2653248 A1 | 19-04-1991 |
| | | | CA | 2027344 A1 | 14-04-1991 |
| | | | DE | 69014817 D1 | 19-01-1995 |
| | | | DE | 69014817 T2 | 22-06-1995 |
| | | | EP | 0423035 A1 | 17-04-1991 |
| | | | ES | 2066169 T3 | 01-03-1995 |
| | | | JP | 1884135 C | 10-11-1994 |
| | | | JP | 3241463 A | 28-10-1991 |
| | | | JP | 6009051 B | 02-02-1994 |
| | | | KR | 147360 B1 | 01-12-1998 |
| US 3696335 | A | 03-10-1972 | US | 3812461 A | 21-05-1974 |
| | | | US | 3940795 A | 24-02-1976 |
| WO 0008610 | A | 17-02-2000 | WO | 0008610 A1 | 17-02-2000 |
| EP 0427465 | A | 15-05-1991 | US | 5120939 A | 09-06-1992 |
| | | | CA | 2023872 A1 | 10-05-1991 |
| | | | DE | 69016589 D1 | 16-03-1995 |
| | | | DE | 69016589 T2 | 07-09-1995 |
| | | | EP | 0427465 A2 | 15-05-1991 |
| | | | JP | 1921556 C | 07-04-1995 |
| | | | JP | 3158955 A | 08-07-1991 |
| | | | JP | 6052518 B | 06-07-1994 |
| EP 0378349 | A | 18-07-1990 | US | 4908521 A | 13-03-1990 |
| | | | AT | 110868 T | 15-09-1994 |
| | | | AU | 613574 B2 | 01-08-1991 |
| | | | AU | 4708389 A | 19-07-1990 |
| | | | CA | 2007234 A1 | 10-07-1990 |
| | | | DE | 69011877 D1 | 06-10-1994 |
| | | | DE | 69011877 T2 | 20-04-1995 |
| | | | EP | 0378349 A2 | 18-07-1990 |
| | | | ES | 2063911 T3 | 16-01-1995 |
| | | | JP | 2226362 A | 07-09-1990 |
| | | | JP | 2714869 B2 | 16-02-1998 |
| | | | NO | 900103 A | 11-07-1990 |

# RAPPORT DE RECHERCHE INTERNATIONALE

de internationale No
PCT/FR 03/00112

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F7/10

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 H04L G07F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie * | Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents | no. des revendications visées |
|---|---|---|
| X | US 5 191 193 A (LE ROUX JEAN-YVES)<br>2 mars 1993 (1993-03-02)<br>abrégé<br>colonne 1, ligne 24 -colonne 2, ligne 42<br>colonne 3, ligne 38 -colonne 4, ligne 51<br>colonne 5, ligne 30 - ligne 35<br>colonne 5, ligne 52 -colonne 6, ligne 2<br>figures 1,2<br>--- | 1,2,6 |
| Y | US 3 696 335 A (LEMELSON JEROME H)<br>3 octobre 1972 (1972-10-03)<br>abrégé<br>colonne 2, ligne 23 -colonne 3, ligne 44<br>colonne 12, ligne 4 - ligne 15<br>figure 1<br>---<br>-/-- | 1-4,6 |

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
"E" document antérieur, mais publié à la date de dépôt international ou après cette date
"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention
"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément
"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier
"&" document qui fait partie de la même famille de brevets

| Date à laquelle la recherche internationale a été effectivement achevée | Date d'expédition du présent rapport de recherche internationale |
|---|---|
| 15 mai 2003 | 26/05/2003 |

| Nom et adresse postale de l'administration chargée de la recherche internationale | Fonctionnaire autorisé |
|---|---|
| Office Européen des Brevets, P.B. 5818 Patentlaan 2<br>NL - 2280 HV Rijswijk<br>Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,<br>Fax: (+31-70) 340-3016 | Dujardin, C |

Formulaire PCT/ISA/210 (deuxième feuille) (juillet 1992)

# RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/00112

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

| Catégorie * | Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents | no. des revendications visées |
|---|---|---|
| Y | WO 00 08610 A (MICROSOFT CORP)<br>17 février 2000 (2000-02-17)<br>abrégé<br>page 9, ligne 21 -page 11, ligne 3<br>page 11, ligne 24 -page 12, ligne 7<br>page 12, ligne 23 -page 19, ligne 2<br>figures 1-5 | 1-4,6 |
| A | EP 0 427 465 A (AMERICAN TELEPHONE & TELEGRAPH) 15 mai 1991 (1991-05-15)<br>abrégé<br>colonne 5, ligne 4 - ligne 50<br>colonne 6, ligne 54 -colonne 7, ligne 11<br>figure 1 | 1,2,6 |
| A | EP 0 378 349 A (VISA INT SERVICE ASS)<br>18 juillet 1990 (1990-07-18)<br>abrégé<br>page 3, ligne 19 -page 4, ligne 12<br>page 5, ligne 22 - ligne 49<br>page 13, ligne 4 - ligne 20 | 1,2,6 |

## RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale No
PCT/FR 03/00112

| Document brevet cité au rapport de recherche | | Date de publication | Membre(s) de la famille de brevet(s) | | Date de publication |
|---|---|---|---|---|---|
| US 5191193 | A | 02-03-1993 | FR | 2653248 A1 | 19-04-1991 |
| | | | CA | 2027344 A1 | 14-04-1991 |
| | | | DE | 69014817 D1 | 19-01-1995 |
| | | | DE | 69014817 T2 | 22-06-1995 |
| | | | EP | 0423035 A1 | 17-04-1991 |
| | | | ES | 2066169 T3 | 01-03-1995 |
| | | | JP | 1884135 C | 10-11-1994 |
| | | | JP | 3241463 A | 28-10-1991 |
| | | | JP | 6009051 B | 02-02-1994 |
| | | | KR | 147360 B1 | 01-12-1998 |
| US 3696335 | A | 03-10-1972 | US | 3812461 A | 21-05-1974 |
| | | | US | 3940795 A | 24-02-1976 |
| WO 0008610 | A | 17-02-2000 | WO | 0008610 A1 | 17-02-2000 |
| EP 0427465 | A | 15-05-1991 | US | 5120939 A | 09-06-1992 |
| | | | CA | 2023872 A1 | 10-05-1991 |
| | | | DE | 69016589 D1 | 16-03-1995 |
| | | | DE | 69016589 T2 | 07-09-1995 |
| | | | EP | 0427465 A2 | 15-05-1991 |
| | | | JP | 1921556 C | 07-04-1995 |
| | | | JP | 3158955 A | 08-07-1991 |
| | | | JP | 6052518 B | 06-07-1994 |
| EP 0378349 | A | 18-07-1990 | US | 4908521 A | 13-03-1990 |
| | | | AT | 110868 T | 15-09-1994 |
| | | | AU | 613574 B2 | 01-08-1991 |
| | | | AU | 4708389 A | 19-07-1990 |
| | | | CA | 2007234 A1 | 10-07-1990 |
| | | | DE | 69011877 D1 | 06-10-1994 |
| | | | DE | 69011877 T2 | 20-04-1995 |
| | | | EP | 0378349 A2 | 18-07-1990 |
| | | | ES | 2063911 T3 | 16-01-1995 |
| | | | JP | 2226362 A | 07-09-1990 |
| | | | JP | 2714869 B2 | 16-02-1998 |
| | | | NO | 900103 A | 11-07-1990 |